REMARKS/ARGUMENTS

Claims

The Examiner rejected claims 1-6, 8-38, 40-69, and 71-81. By this amendment, claims 1, 33, and 65 have been amended, and claims 2, 34 and 66 have been cancelled. Therefore claims 1, 3-6, 8-33, 35-38, 40-65, 67-69, and 71-81 remain pending in the application.

Claim Rejections – 35 USC § 103

Claims 1, 2, 11, 33, 34, 43, 65, 66, and 71 were rejected under 35 USC 103(a) as being unpatentable over Sekendur (USPN 5,852,434) in view of Patel (USPN 5,857,029) in view of Khan et al. (USPN 6,401,206, newly cited) hereinafter Khan. The rejection is respectfully traversed.

In the Advisory Action mailed February 19, 2004, the Examiner appeared to agree that all of the previously cited references do not disclose the "signature key" of independent claims 1, 33 and 65 when it is interpreted narrowly as a private key. Therefore such an explicit limitation of the term "signature key" was made in the Applicants' next response. Nevertheless, in the present office action the Examiner has cited new art by Khan and asserted that the independent claims are still obvious.

Khan appears to be of no particular relevance as it merely discloses the typical use of a digital signature of digital content related to computer software that is generated in a computer system using a private signature key of a user. The Applicants respectfully assert that the present invention is still non-obvious in view of Khan because of the claimed combination of a secure sensing device and a digital signature.

However, to clarify the distinctions between the cited prior art and the present invention, the present independent claims have been amended to explicitly state that the sensing device is linked, during a registration process, to an authorized user using a secret key-exchange key and first digital ink consisting of the authorized user's handwritten signature. Further the movement data are explicitly limited to representing second digital ink consisting of a user's handwritten signature. Finally, an explicit verification step has been added of verifying the user's handwritten signature by comparing the second digital ink with the first digital ink.

The present invention thus claims redundant levels of computer system security by including a secure (registered) sensing device that is linked to an authorized user during a registration process, comparison of digital ink for signature verification, and the generation of a secure digital signature. Use of such redundant levels of security is neither disclosed nor fairly suggested by the prior art cited by the Examiner.

Support for the present amendments is found, for example, in the specification as originally filed at page 22, lines 8-12, where the sensing device of the present claims is referred to as a "pen":

> *"The netpage registration server 11 is a server which records relationships between users, pens, printers, applications and publications, and thereby authorizes various network activities. It authenticates users and acts as a signing proxy on behalf of authenticated users in application transactions. It also provides handwriting recognition services."*

Further support for the present amendments is found, for example, in the specification as originally filed at page 52, lines 5-21:

"In addition to its public ID, the pen contains a secret key-exchange key. The key-exchange key is also recorded in the netpage registration server database at time of manufacture...When a previously unregistered pen is first registered, it is of limited use until it is linked to a user. A registered but "un-owned" pen is only allowed to be used to request and fill in netpage user and pen registration forms, to register a new user to which the new pen is automatically linked, or to add a new pen to an existing user.

The pen uses secret-key rather than public-key encryption because of hardware performance constraints in the pen."

Still further support for the present amendments is found, for example, in the specification as originally filed at page 32, line 28, to page 33, line 3:

"A signature field has an associated digital signature value 883, as shown in Figure 37. Any digital ink captured in a signature field's zone is automatically verified with respect to the identity of the owner of the pen, and a digital signature of the content of the form of which the field is part is generated and assigned to the field's value. The digital signature is generated using the pen user's private signature key specific to the application which owns the form."

The Applicants respectfully assert that the rejections of the dependent claims are now moot in light of the present amendments to the independent claims.

The present amendments have therefore clearly limited the claims to systems and methods including a secure sensing device, comparison of digital ink for signature verification, and the generation of a secure digital signature, thereby providing added system security. None of the references cited by the Examiner disclose or fairly suggest the claimed combination of such limitations. Accordingly, it is submitted that the application is now in condition for allowance. Reconsideration and allowance of the application is courteously solicited.

Very respectfully,

Applicants:

KIA SILVERBROOK

PAUL LAPSTUN

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia
Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762